IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No. 10/685,234
Filing Date 10/14/2003
First Named Inventor ..... Bin Zhu
Assignee ..... Microsoft Corporation
Group Art Unit 2134
Examiner ..... Matthew Heneghan
Attorney's Docket No. MS1-1753US
Title ..... Digital Rights Management System

DECLARATION UNDER 37 CFR §1.132

To: Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

From: Kasey Christie (Tel. 509-324-9256; Fax 509-323-8979)
Customer No. 22801

On behalf of the Microsoft Corporation, this declaration and the attached exhibit A is submitted as proof that the changes effected by the Applicant's communication with the U.S. Patent and Trademark Office dated November 25, 2003 and titled "Preliminary Amendment" do not constitute the impermissible introduction of "new matter." The changes in the Preliminary Amendment are not new matter because each change is merely a correction or a clarification that would be recognized as such by one or ordinary skill in the art.

Indeed, I hereby declare each of the changes in the Preliminary Amendment are not new matter because each change is merely a correction or a clarification that would be recognized as such by one or ordinary skill in the art.

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

10/7/2007
Date

Min Feng
Min Feng

MIN FENG
Printed name/Title

Hi, Kasey

Here are my comments about Bin's patent's change from A to E. Please see the comments injected among change descriptions.

Best Regards!

Min FENG
Tel: +86(10)58963453
Internet Media Group
Microsoft Research Asia

Exhibit A

From: Kasey Christie
Sent: Monday, August 06, 2007 9:00 AM
To: 'Min FENG'
Cc: PLaw; Carly Bokarica
Subject: MS#306096.01 MS1-1753US | Seeking expert advice

Min:

Thank you for your help. In order to prepare for that declaration, can I get you to explain each of the changes? I will list each one below. There are 5 of them (changes A-E).

Please mark your in-line comments with preceeding "[Min]"

Note that the ~~crossed-out text~~ represents deletions and underlined text represents additions.

Change A

[0050] The content publisher generates the sharing polynomial $f(x)$ ~~over a finite field Z_N~~ where $a_o = SK$. Although polynomial interpolation is described, other collections of functions may also be utilized. Each partial secret share S_i may then be calculated using Equation (3), which is shown as follows:

$$S_i = f(id_i) \bmod \cancel{N}\ \phi(N) \qquad (3)$$

where N is an RSA modulus and $\phi(N)$ is an Euler totient function.

[Min] For the part 2: According to number theory, for any arbitrary integer α between 1 and N-1, $\alpha^{\phi(N)} = 1 \bmod N$. So any operations such as addition, subtraction, multiplication and division on the exponent position should mod $\phi(N)$ instead of N. The result of $f(x)$ is used on the exponent position of the operation $a^x \bmod N$, so the result of the polynomial $f(x)$ should mod $\phi(N)$.

For the part 1: First since N is a compound number, Zn is definitely not a finite field. So any operations such as addition, subtraction, multiplication and division on the exponent position should mod $\phi(N)$. $f(x)$ can be said that it is defined over Z_n^* not Zn, but any polynomial in $Z[x]$

(coefficients are in Z) can be regarded as a polynomial in $Z_n^*[x]$ by mapping the coefficients $a_i \rightarrow a_i \bmod \phi(N)$.

These errors can be detected and corrected by any one learn some number theory. They are some kind of typo. The changes are correct.

Change B

[0053] At block 514, for instance, the content publisher may broadcast k public witnesses of the sharing polynomial's coefficients, which are denoted as $\{g^{a_0}, \ldots, g^{a_{k-1}}\}$, where $g \in Z_N$ $g \in Z_N^*$. After broadcast, the content publisher may destroy the polynomial. At block 516, each license authority id_i verifies validity of the received partial secret share. Validity may be checked by determining if Equation (4), as shown below, holds for the received partial secret share S_i utilizing the sharing polynomial's coefficients which were broadcast at block 514:

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \quad \underline{\text{mod N}} \qquad (4)$$

In this way, each license authority id_i, may verify the validity of the received partial secret share S_i without exposing or knowing the secret, i.e. the private key SK.

[Min] For part 1: $g \in Z_n^*$ makes g has a large order which equals to $\phi(N)$ for the cyclic group g itself generates. $g \in Z_n$ can also be OK if g is randomly chosen from Zn, and has no influence on other equations and formulas. Only a small number of $g \in Z_n$ has an order less than $\phi(N)$.

For part 2: It is really good that the authors explicitly describe the equation is computed by "mod N" . $g \in Z_n^*$ is also an element in Zn (Z_n^* is a subset of Zn). So the final result is "mod N". People in my field will assume the operation is "mod N" as default.

While these changes may not be regarded exactly as errors. The changes make the scheme more clear and solid.

Change C

[0063] At block 620, the content player, when executed by the client device, determines if k correct partial

licenses have been received by validating each of the partial licenses. The partial licenses may be validated as follows. First, node p calculates

$$g^{S_I} = g^{a_0} \cdot (g^{a_1})^{id_I} \cdot \ldots \cdot (g^{a_{k-1}})^{id_I^{k-1}} \quad \underline{\text{mod } N} \qquad ((7)$$

from the public witnesses of the sharing polynomial's coefficients, as was described in relation to block 516 of FIG. 5 and Equation (4). Equation (6) is then applied to g^{S_i} and the received partial license $prel_i$, A_1, and A_2 to calculate c. The received partial license $prel_i$ is verified by checking if the following equations hold: $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$. The above steps are repeated until the node p obtains k valid partial licenses. If k valid partial licenses cannot be obtained, generation of the formal-license fails (block 622).

[Min] It is really good that the authors explicitly describe the equation is computed by "mod N". People in my field will assume the operation is "mod N" as default. This change might not be regarded as an error. The change makes the scheme more clear.

Change D

[0064] If k valid partial licenses are obtained, then at block 624, the content player combines the partial licenses to form the formal license. For example, the node p uses the k valid partial results to calculate the formal license utilizing Equation (8):

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)} \qquad ((8)$$

$$= (prel)^{SK} = ((license)^{PK})^{SK} \quad \underline{\text{mod } N,}$$

where $l_{id_i}(x) = \prod_{j=1, j \neq i}^{k} \frac{x - id_j}{id_i - id_j}$.

[Min] Again, it is really good that the authors explicitly describe the equation is computed by "mod N". People in my field will assume the operation is "mod N" as default. This change may not be regarded as an error. The change makes the scheme more clear.

Change E

[0075] At periodic intervals, for example, the license authorities may update their respective shares of the

private key *SK* through execution of the respective update module 222 of FIG. 2. At block 802, each license authority *i* generates a random *(k, m)* sharing of the secret *0* using a random update polynomial $f_{i, update}(x)$, as shown in Equation (9):

((9)

$$f_{i,update}(x) = b_{i,1}x + \_ + b_{i,k-1}x^{k-1} \bmod N$$

[Min]"mod N" is definitely wrong. Because the result of $f_{i,update}(x)$ is used as the exponent value in the operation of $a^x \bmod N$. So the result of the polynomial $f_{i,update}(x)$ should be mod $\phi(N)$. I suggest that "mod $\phi(N)$" be added explicitly at the end of Equation 9 to avoid misunderstanding.

In addition, the authors should also explicitly state in the patent application that
1) $\phi(N)$ is public
2) PK is not disclosed
The current version does not mention explicitly the above conditions in the patent application. They are implicitly used to make the whole system work. Stating them explicitly can help readers understand the equations and the whole system.

Thank you.

kasey

Kasey Christie
(509)324-9256 x232
kasey@leehayes.com

Lee & Hayes pllc, Intellectual Property Law
421 West Riverside, Suite 500, Spokane, WA 99201 | 509.323-8979 fax | www.leehayes.com

NOTE: This email and any attachments contain information from the law firm of Lee & Hayes, pllc, that is confidential and/or subject to attorney-client privilege. If you are not the intended recipient of this message, please do not read it or disclose it to others. Instead, please delete it and notify the sender immediately.